UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/788,523	02/27/2004	Atsushi Minemura	36483	6891

116 7590 06/12/2007

PEARNE & GORDON LLP
1801 EAST 9TH STREET
SUITE 1200
CLEVELAND, OH 44114-3108

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
06/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/788,523	MINEMURA, ATSUSHI	
	Examiner	Art Unit	
	Amare F. Tabor	2109	

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 February 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/15/04, 10/25/04 & 05/24/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-11 have been examined.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. P. 2003-053362, filed on 02/28/2003.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 8 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 8 is directed to a computer program per se, which is not tangibly embodied on an appropriate computer readable medium and therefore does not constitute statutory subject matter.

Claims 9 and 10 depend on the rejected claim 8, and include all the limitations of claim 8, thereby rendering those dependent claims non-statutory.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims recite the limitations "secure device" and "application running means." These limitations are vague and broad. The disclosure of the invention explains, "secure device" and "application running means" as "IC card, or the like" (page 1, lines 19-20) and "JAVA Runtime Environment/JAM" (page 7, lines 21-22) respectively. Therefore, the examiner interpreted the above respective limitations as "Integrated Circuit/IC Card" and "Runtime Environment," for examining purpose.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1 and 11 are rejected under 35 U.S.C. 102(b) as being anticipated by Deo et al. (US Patent No. 5,721,781 A, cited by the applicant), referred as "Deo" hereinafter.

6. As per claim 1 and 11, Deo discloses,

An application authentication system comprising: (abstract, lines 1, "**an authentication system** includes")

- a terminal device having no secure information area, said terminal device including an application and application running means; (abstract, lines 8-12, "the system further includes **a terminal** that is capable of accessing the smart card. The terminal has at least one compatible **application** which operates in conjunction with the application on the smart card"). Thus, the system includes an inherent application running means. And Deo further disclose the "no secure information area" as "unsecured channel" (figure 4).

- and a secure device connected fixedly or detachably to said terminal device, said secure device for authenticating the application requesting access to the secure device; (abstract, lines 1-3, "a portable information device, **such as a smart card**, that is configured to store and process multiple different applications"). The "secure device" is the "smart card" as claimed. And Deo further disclose the smart card can be connected fixedly or detachably (column 4, lines 43-47).

- wherein said secure device authenticates the application running means, and then authenticates the application based on a result of that the application running means execute a process on the application (abstract, lines 16-21, "during transactional session, the smart card and terminal exchange their certificates to authenticate one another. Thereafter, **a smart card application is selected** and the related certificates for both the smart card application and the terminal application are exchanged between the smart card and terminal to **authenticate the applications**"). Therefore, it is the smart card; i.e., the secure device as claimed, which authenticates the application running means and the application.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deo in view of Wentker et al. (US Patent No. 6,481,632 B1, this reference is also cited by the applicant), referred as "Wentker" hereinafter.

8. *As per claim 2*, Deo discloses,

Attaching and verifying the electronic signature to an application as, (column 7, lines 14-16, "when smart card encrypts a message using the terminal's public key, it **tags** a personalized **digital signature** on to the message. The smart card **encrypts the combined message** using its own private key"). The "digital signature" is the "electronic signature" as claimed.

However, Deo does not explicitly disclose,

- wherein the application running means calculates digest data of the application to which an electronic signature is attached, and presents the digest data and the electronic signature to the secure device

On the other hand, in the same field of endeavor, Wentker discloses, (column 15, lines 19-20 and 23-26, "in step 342 creation of a data authentication pattern/DAP may be performed in a variety of ways," and "by **calculating a DAP for an application**, for example, and delivering the DAP with the application, an entity such as a smart card can recalculate the DAP using the same cryptographic technique"). The "DAP" is the "digest" as claimed.

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of calculating the DAP as per teachings of Wentker to the process of verifying the electronic signature as taught by Deo in order to provide security domain between the card manager and the application programming interface/API (see Wentker fig. 3).

- and the secure device verifies the electronic signature by using the presented digest data, and then authenticates the application if a verified result is normal

Wintker further discloses, (column 15, lines 61-67, "the private key is used to **sign** a cryptographic hash of the command or the application which then becomes the unique DAP. The issuer's

public key held by the card manager is used to verify the DAP received along with either a command or an application. That is, **the smart card** uses the issuer's public key to **verify the DAP for the application**").

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of verifying the DAP as per teachings of Wentker into authentication of applications as taught by Deo in order to allow load, install and/or delete an application (see Wentker column 12, lines 1-4).

9. *As per claim 3*, rejection of claim 2 is incorporated.

However, Deo does not explicitly disclose,

- wherein the application running means calculates digest data of the application and presents the digest data to the secure device, and the secure device collates the presented digest data with digest data held in a database of the secure device, and then authenticates the application if a collated result is normal

On the other hand, Wentker discloses, (column 15, lines 41-49, "the DAP may then be **appended** to the clear text of the information for transmission. On the receiving end, for example inside the smart card, the application (for example) and its appended DAP are received. Next, the same technique is applied to the application using the same cryptographic algorithm as before to produce a new DAP for the application. Assuming the application has not been changed enroute, the newly created DAP **should match** the DAP received appended to the application"). The appended DAPs are the database as claimed and the matching process confirms the collated result is normal; moreover, the process of authenticating the application is disclosed as, "a difference in the two DAPs will indicate that **the integrity of the application** has been compromised" (column 15, lines 49-51).

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of appending the calculated DAP as per teachings of Wentker into the process of authenticating an application as taught by Deo in order to test and certify the correctness of an application (see Wentker column 15, lines 15-19).

10. *As per claim 4*, rejection of claim 3 is incorporated and further Deo discloses,

wherein the secure device sends out first information to the application running means,

(figure 5 and column 3 lines 7-9, "during a transactional session, the smart card and the terminal **exchange their certificates** over an unsecured communication path"). The "certificate" is the "first information" as claimed.

However, Deo does not explicitly disclose,

- then wherein the application running means encrypts the first information by using the digest data and sends out encrypted information to the secure device; on the other hand Wintker discloses,(column 7, lines 27-30, "the MAC creation key is used to calculate DAPs for (a) verifying the integrity of data in a command data field and (b) verifying the authenticity of a command").

Wintker further disclose,

- and then the secure device decrypts the first information by using the digest data stored in a database of said secure device and then collates decrypted information with the first information (column 7, lines 30-31, "the key encryption key used to **decrypt keys** that are received by the card") and (column 7, lines 33-37, "in addition to the symmetric key set, the card manager may make use of a asymmetric cryptography by also including the public key of an issuer for decrypting information that has been originally been encrypted using the private key of the issuer").

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of appending the calculated DAP as per teachings of Wentker into the process of exchanging certificates for the authentication of an application as taught by Deo in order to certify the application (see Wentker column 15, lines 15-19).

11. *As per claim 5*, Deo discloses,

wherein the application running means verifies an electronic signature of the application to which the electronic signature is attached to authenticate the application, (column 10, lines 4-7, "the smart card and the terminal **authenticate each other** based upon the information and digital signature contained in their exchanged certificates").

- and the secure device accepts an authenticated result of the application running means to authenticate the application (column 10, lines 13-16, "at step 120, the card holder enters his/her PIN at the terminal. The PIN is passed from the terminal to the smart card so that the smart card can **authenticate the user**."). And Deo further disclose authentication of application as, (column 10, lines 22-26, "the identity information and digital signatures of the certifying authority contained in the certificates are used to **authenticate each application**").

12. *As per claim 6*, Deo discloses,

wherein the secure device 1) shares a second information with the application running means if the secure device authenticates the application running means, (figure 6 and column 9, lines 29-32, "during the authentication phase, the user is requested to enter his/her **PIN** 50 via input

keypad 36. Terminal 32 **passes PIN 50 directly to the smart card** 10 so that it can verify the identity of the cardholder"). The "second information" is the "PIN" as claimed.

2) and accepts process request if the second information are added to the process request issued from the application that the secure device authenticates (column 9, lines 32-35, "the smart card compares the entered PIN with a stored PIN that associated with the true cardholder. If the entered PIN matches, the user is deemed authentic to the smart card").

13. *As per claim 7*, Deo discloses,

A secure device connected fixedly or detachably to a terminal device, said secure device comprising: (see abstract as applied to rejection of claim 1 above).

However, Deo does not explicitly disclose,

- a card manager for executing a process of authenticating the terminal device; on the other hand, Wentker discloses, (column 6, lines 48-52, "**card manager** 104 is a software application that represents the card issuer. It manages run-time environment for applications and controls the overall system and **security for the smart card**").

- and a card application for applying an authenticating process to an access request application stored in the terminal device; Wentker further discloses, (column 6, lines 63-67, "additionally, card manager **loads** issuer application 112") and (column 7, line 9, "card manager 104 can also function as an application").

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of authenticating the terminal by the card manager as per teachings of Wentker into the storing multiple applications as taught by Deo in order to grant access to the API (see Wentker column 6, lines 52-55).

- wherein the card application authenticates the application based on a process that is applied to the application by the terminal device, then confirms that the process of authenticating the terminal by the card manager is completed, and then accepts an access request of the authenticated application. Wentker further discloses, (column 7, lines 15-19, "card manager 104 is responsible for **overall card security** and includes the security domain application of the card issuer which supports key handling, encryption, decryption, signature generation and verification for the card issuer's applications).

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of completing the authentication process by the card manager as per teachings of Wentker into processing multiple applications as taught by Deo in order to identify specific applications (see Wentker column 7, lines 15-18).

14. *As per claim 8*, Deo discloses,

A terminal device including: an application running means; and an application, (see abstract as applied to rejection of claim 1 above).

However, Deo does not explicitly disclose,

- wherein the application running means calculates digest data of the application to request access to a secure device after the fitted secure device authenticates the application running means, then authenticates the application by using the digest data, and then issues an access request to the secure device (column 12, lines 49-57, "the card issuer pre-authorizes the initial install command (which performs loading) and the load file through the use of these data authentication patterns. The data authentication pattern for the application file is included in the initial Install command to ensure that application which has been approved by the card issuer is the same application that is subsequently received by the card manager through the series of loading commands that follow the first install command").

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of using calculated DAP to load applications as per teachings of Wentker into the process of authenticating an application as taught by Deo in order to certify the application (see Wentker column 15, lines 15-19).

15. *As per claim 9*,

This claim has the limitations that is similar to those of claim 2, thus is rejected with the same rationale applied against claim 2 above.

16. *As per claim 10*,

This claim has the limitations that is similar to those of claim 3, thus is rejected with the same rationale applied against claim 3 above.

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

TITLE: IC card terminal US 6,866,192 B2

TITLE: Biometric authentication system US 6,219,439 B1

TITLE: Smart card pin system, card, and reader US 6,257,486 B1

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare F. Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on (571) 270-1392. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AFT

Chameli Das
CHAMELI DAS
SUPERVISORY PATENT EXAMINER
6/8/07